IN THE SPECIFICATION

Please amend the specification as follows.

Paragraph [0019] is amended as follows:

Unlike X.509 identity certificates, SPKI authorization certificates do not need CAs and do not require Certificate Revocation Lists (CRLs). A CRL is a mechanism that a CA uses to publish and disseminate information about revoked certificates to certificate-issuers. A CRL is analogous to a list of bad checking accounts maintained by a grocery store. Maintaining and publishing notices of revoked certificates is widely acknowledged to be expensive and problematic. One aspect of the present invention is a method where an intermediary, e.g. a client, issues a long-lived [[SKPI]] SPKI authorization certificate to a third party so that the validity of the certificate and corresponding potential for harm is implicitly limited by the subsequent involvement of the intermediary in the certificate processing. This increases security in cases where services are outsourced across organizational boundaries where trust relationships are less stable than in traditional business models.

Paragraph [0027] is amended as follows:

As shown in Figure 8, another aspect of the present invention is a machine-accessible medium having associated content capable of directing the machine to perform a method of assembling authorization certificate chains among an authorizer, a client, and a third party 800. In one embodiment, the associated content is a software development kit. The client receives a first certificate from the authorizer 802 and then generates a URI associated with both the at least one first certificate and the third party 804. The client provides a second certificate and the URI to the third party 806. After the third party provides the second certificate and URI to the authorizer 808, the authorizer ~~aecess~~ accesses the URI 810 and, then, the client provides the first certificate to the authorizer 812. In one embodiment, the third party provides the second certificate and URI to the authorizer in an XML signature. In another embodiment, the first and

second certificates are SPKI certificates. In another embodiment, the authorizer grants access to the third party. In another embodiment, the client tracks at least one use of the second certificate. In another embodiment the client revokes the second certificate.

Paragraph [0030] is amended as follows:

It is to be understood that the above description [[it]] is intended to be illustrative, and not restrictive. Many other embodiments are possible and some will be apparent to those skilled in the art, upon reviewing the above description. For example various types of digital certificates may be used in place of SPKI certificates, languages other than XML may be used, communications other than SOAP requests may be used, Universal Resource Locators (URLs) may be used in place of URIs, Intranets, Local Area Networks (LANs) or other networks may be used in place of the Internet, and more. Therefore, the spirit and scope of the appended claims should not be limited to the above description. The scope of the invention should be determined with reference to the appended claims, along with the full scope of equivalents to which such claims are entitled.